UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/809,111	03/25/2004	Jonathan Wilkins	MS#307312.01 (5104)	6640

38779 7590 09/15/2008
SENNIGER POWERS LLP (MSFT)
100 NORTH BROADWAY
17TH FLOOR
ST. LOUIS, MO 63102

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2139	

NOTIFICATION DATE	DELIVERY MODE
09/15/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspatents@senniger.com

Office Action Summary	Application No.	Applicant(s)	
	10/809,111	WILKINS ET AL.	
	Examiner	Art Unit	
	CHRISTIAN LAFORGIA	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 June 2008*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-24 and 26-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-24 and 26-40* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 March 2004* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)	4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)	5) □ Notice of Informal Patent Application
3) □ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.	6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 23 June 2008 has been entered.

2. Claims 1-3, 5-24, and 26-40 have been presented for examination.

3. Claims 4 and 25 have been cancelled as per Applicant's request.

Response to Arguments

4. Applicant's arguments with respect to claims 1-3, 5-24, and 26-40 have been considered but are moot in view of the new grounds of rejection set forth below.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-3, 5-10, 15-19, 21, 22, 26-30, and 32-38 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application Publication No. 2004/0255155 A1 to Stading, hereinafter Stading.

7. As per claims 1, 15, 16, 26, 30, 32, and 33, Stading discloses a method of detecting an attack on an authentication service (abstract, title), said method comprising:

storing data relating to a plurality of requests as communicated to an authentication service from a plurality of user agents via a data communication network, said requests each including a password (Figure 1 [element 118], paragraph 0032, i.e. storing user passwords in usual password files), and wherein storing the data relating to the requests comprises storing the password of each of the requests only if the request is unsuccessful (paragraphs 0036, 0037, 0041, i.e. storing alert passwords in tables, alert passwords are evidenced by failures of submitted passwords and are brought into use to detect an attack);

searching the stored data based on a query variable to identify at least one of the plurality of the requests communicated from at least one of the plurality of the user agents (paragraph 0038, i.e. receiving a password and comparing it to the password tables),

comparing the stored data associated with the identified request with a predefined pattern characterizing an attack based on the stored password of the identified request to determine when the identified request indicates the characterized attack on the authentication service (paragraph 0038, i.e. receiving a password and comparing it to the password tables); and

detecting the attack in response to determining that the identified request indicates the characterized attack (paragraphs 0038, 0039, i.e. detecting an alert password, thereby detecting an attack).

8. Regarding claims 2, 17, 27, and 34, Stading discloses wherein said storing the data relating to the plurality of the requests comprises storing one or more of the following:

a network address from which one of the plurality of the requests is communicated; a credential type of the one of the plurality of the requests; a user account associated with the one of the plurality of the requests; a status of the one of the plurality of the requests; a time stamp indicating a date and time of the one of the plurality of the requests; a type of interface from which the one of the plurality of the requests is communicated; and the user agent from which the one of the plurality of the requests is communicated (paragraph 0039, i.e. tracking, logging, notifying, tracing and identifying an attacker).

9. With regards to claim 3, Stading discloses wherein said status of the one of the plurality of the requests comprises one or more of the following: the one of the plurality of the requests is successful; the one of the plurality of the requests is unsuccessful (paragraphs 0038, 0039, i.e. user logs in with the correct password and is therefore successful or the user logs in with an alert password or incorrect password and is therefore unsuccessful); and the user account associated with the one of the plurality of the requests has been locked.

10. Regarding claim 5, Stading teaches wherein said comparing the stored data associated with each of the identified requests with the predefined pattern comprises comparing the stored data with a pattern characterized by one or more of the following: using a single password to unsuccessfully attempt at least a predetermined quantity of requests on multiple user accounts within a predefined time interval (paragraph 0035, i.e. dictionary attacks use the same set of passwords to attack multiple user accounts); using the single password to unsuccessfully attempt at least the predetermined quantity of the requests from a single network address on the multiple

user accounts within the predefined time interval; and unsuccessfully attempting at least the predetermined quantity of the requests from the single network address within the predefined time interval.

11. Regarding claims 6 and 19, Stading teaches wherein said comparing the stored data associated with each of the identified requests with the predefined pattern comprises comparing the stored data with a pattern characterized by one or more of the following: using multiple passwords to unsuccessfully attempt at least a predetermined quantity of requests on a single user account within a predefined time interval (paragraph 0035, i.e. dictionary attacks are using multiple passwords to try and get into a single user account); using the multiple passwords to unsuccessfully attempt at least the predetermined quantity of the requests from a single network address on the single user account within the predefined time interval; and unsuccessfully attempting at least the predetermined quantity of the requests on the single user account within the predefined time interval.

12. Regarding claims 7, 18, 28 and 35, Stading teaches wherein said comparing the stored data associated with each of the identified requests with the predefined pattern comprises comparing the stored data with a pattern characterized by one or more of the following: a single password to unsuccessfully attempt at least a predetermined quantity of requests from multiple network addresses on a single user account within a predefined time interval (paragraph 0035, i.e. dictionary attacks use the same set of passwords to attack multiple user accounts); and

unsuccessfully attempting at least the predetermined quantity of the requests from the multiple network addresses on the single user account.

13. Regarding claims 8, 21, 29, 36, Stading discloses generating a report if it is determined that one or more of the identified requests indicate the characterized attack, said report providing information regarding the attack for use in defending against the attack (paragraph 0039, i.e. logging).

14. Regarding claims 9, 22, and 37, Stading discloses remedying the attack if it is determined that one or more of the identified requests indicate the characterized attack (paragraph 0039, i.e. logging attacker into a honeypot).

15. With regards to claims 10 and 38, Stading discloses wherein said remedying the attack comprises performing one or more of the following: locking a user account associated with one of the plurality of the requests; blocking a network address from which the one of the plurality of the requests is communicated; implementing a human interaction proof on the authentication service; prompting a user to change a password associated with the user account (paragraph 0059); and limiting a quantity of allowed unsuccessful requests to a predetermined quantity within a predefined time interval for the network address from which the one of the plurality of the requests is communicated.

Claim Rejections - 35 USC § 103

16. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

17. Claims 11, 12, 23, 24, 31, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stading in view of U.S. Patent Application Publication No. 2002/0097145 to Tumey et al., hereinafter Tumey.

18. Regarding claims 11 and 23, Stading teaches wherein the plurality of the requests comprises one or more of the following types of requests:

authentication, registration, and password-reset (paragraph 0059).

19. Stading does not teach wherein one of the plurality of the requests is communicated via a human interaction proof; and wherein said storing the data relating to the plurality of the requests comprises storing one or more of the following: a network address from which the one of the plurality of the requests is communicated, a process where the human interaction proof is implemented, a time stamp indicating a date and time of the one of the plurality of the requests, and the user agent from which the one of the plurality of the requests is communicated.

20. Tumey teaches wherein said storing the data relating to the plurality of the requests comprises storing one or more of the following: a network address from which the one of the plurality of the requests is communicated, a process where the human interaction proof is implemented, a time stamp indicating a date and time of the one of the plurality of the requests, and the user agent from which the one of the plurality of the requests is communicated

(paragraph [0033] where the human facial image data is interpreted to be the human interaction proof used for authentication).

21. It would be obvious to one of ordinary skill in the art at the time of invention to use the biometric security of Tumey, since Tumey states at paragraph 0005 that facial recognition is noninvasive security to the user and effective at all times, thereby providing for a more secure system.

22. Regarding claims 12, 24, 31, and 39, Stading does not teach wherein said comparing the stored data associated with each of the identified requests with the predefined pattern comprises comparing the stored data with a pattern characterized by one or more of the following: using multiple test strings to unsuccessfully attempt at least a predetermined quantity of requests on a single human interaction proof string within a predefined time interval; and using a single test string to unsuccessfully attempt at least the predetermined quantity of the requests on multiple human interaction proof strings within the predefined time interval.

23. Tumey teaches wherein said comparing the stored data associated with each of the identified requests with the predefined pattern comprises comparing the stored data with a pattern characterized by one or more of the following: using multiple test strings to unsuccessfully attempt at least a predetermined quantity of requests on a single human interaction proof string within a predefined time interval; and using a single test string to unsuccessfully attempt at least the predetermined quantity of the requests on multiple human interaction proof strings within the predefined time interval (paragraphs 0070, 0071).

24. It would be obvious to one of ordinary skill in the art to use multiple images to create a threshold for authentication, since Tumey states at paragraph 0072 that images may have erroneous verification results to do poor presentation of the user to the system's camera and that it is best to create a threshold so as to create the best image for the security of the user.

25. Claims 13, 14, 20, and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stading in view of U.S. Patent Application Publication No. 2003/0145225 A1 to Bruton, III et al., hereinafter Bruton.

26. Regarding claim 13, Stading does not teach wherein said comparing the stored data associated with each of the identified requests with a predefined pattern comprises: comparing historical data relating to the authentication service with the stored data, and in response to said comparing, determining if the stored data deviates from the historical data to determine if the attack on the authentication service has occurred.

27. Bruton discloses wherein said comparing the stored data associated with each of the identified requests with a predefined pattern comprises comparing historical data relating to the authentication service with the stored data, and in response to said comparing, determining if the stored data deviates from the historical data to determine if the attack on the authentication service has occurred (paragraph 0069).

28. It would have been obvious to one of ordinary skill in the art at the time the invention was made to compare historical data relating to the authentication service with the stored data, and in response to said comparing, determining if the stored data deviates from the historical data to determine if the attack on the authentication service has occurred, since Bruton states at

paragraph 0039 that this historical data and statistics is used to establish further intrusion detection policies.

29. Regarding claims 14, 20, and 40, Stading does not teach wherein said searching the stored data to identify at least one of the plurality of the requests comprises searching the stored data to generate a result set based on one or more of the following query variables: a network address that communicates an request, a quantity of user accounts for which access has been attempted, a password associated with a failed request, a quantity of failed requests for one or more user accounts, a quantity of requests for one or more user accounts, and a time interval during which one or more requests are communicated; wherein the result set identifies the stored data relating to one or more requests that correspond to the query variables.

30. Bruton discloses wherein said searching the stored data to identify at least one of the plurality of the requests comprises searching the stored data to generate a result set based on one or more of the following query variables: a network address that communicates an request, a quantity of user accounts for which access has been attempted, a password associated with a failed request, a quantity of failed requests for one or more user accounts, a quantity of requests for one or more user accounts (paragraph 0010), and a time interval during which one or more requests are communicated; wherein the result set identifies the stored data relating to one or more requests that correspond to the query variables (paragraphs 0083, 0084).

31. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the searching the stored data to generate a result set based on one or more of the following query variables: a network address that communicates an request, a quantity of user

accounts for which access has been attempted, a password associated with a failed request, a quantity of failed requests for one or more user accounts, a quantity of requests for one or more user accounts, and a time interval during which one or more requests are communicated; wherein the result set identifies the stored data relating to one or more requests that correspond to the query variables, since Bruton states at paragraph 0084 that searching this way provides for more efficient processing by allowing for optimization.

Conclusion

32. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

33. The following patents are cited to further show the state of the art with respect to detecting a password attack, such as:

United States Patent Application Publication No. 2005/0015614 A1 to Gilfix et al., which is cited to show detecting password attacks using modeling techniques.

United States Patent No. 7,386,892 B2 to Gilfix et al., which is cited to show detecting password attacks using modeling techniques.

34. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

35. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine L. Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

36. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2139

clf